UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/982,624	10/18/2001	Taizo Shirai	450100-03550	8604

20999 7590 03/01/2005

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/982,624	SHIRAI ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/01/2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on February 01, 2002. Claims 1 – 9 were received for consideration. No preliminary amendments to the specification were filed. Claims 1 – 9 are currently being considered.

Specification

2. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed. The following title is suggested: "Data storage with CBC-mode encryption processing"

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1 – 9 are rejected under 35 U.S.C. 102(b) as being anticipated by Michener et al. (U.S. Patent Number 5,671,283).

Regarding Claim 1, Michener teaches and describes a data storage device comprising:

a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity (Column 4 lines 9 – 14); and

cryptosystem means (Column 4 lines 9 – 14);

wherein said cryptosystem means receives, as cryptosystem keys for performing cryptosystem processing on data to be stored in said data storage area a set of keys correlated with the encryption keys or decryption keys for each of the sectors from a device capable of performing data communication with said data storage device, and transmits, to said device, a set of encrypted keys obtained by executing encryption processing in the cipher block chaining (CBC) mode on the received set of keys (Column 4 lines 9 – 31, Column 5 lines 26 – 53 and Column 6 lines 15 – 25). Michener teaches that the crypto system receives a set of keys correlated with the encryption or decryption (transaction, unit and transaction identification) keys for each block.

4. Regarding Claim 6, Michener teaches and describes a data recording method for a data processor comprising:

a data storage device comprising cryptosystem means and a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity (Column 4 lines 9 – 14); and

a data recording device for executing data storage processing by transmitting data to said data storage device, said data recording method comprising the steps of:

executing mutual authentication processing between said data storage device and said data recording device (Column 6 lines 33 – 45 and Column 7 lines 2 – 5), Michener teaches that mutual authentication between the user terminal and the storage with crypto unit;

when the mutual authentication is established, transmitting, to said data storage device, by said data recording device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on said set of keys applicable to encryption processing on pieces of data to be stored in the sectors (Column 6 lines 15 – 61 and Column 7 lines 2 – 5), Michener teaches that when the mutual authentication is established and that the transaction verification (session) keys are generated to be stored in the sectors;

decrypting, by said data storage device, said set of session-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the session key (Column 6 lines 21 – 25 and Column 7 lines 6 - 10);

transmitting, to said data storage device, a set of decrypting, by storage-key-used generated by executing based on a storage key unique to said data storage device, encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode-processing keys (Column 7 lines 6 – 10); and

generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys which are generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys, the header information corresponding to the data to be stored in said data storage device (Column 6 lines 16 – 28 and 48 – 61).

5. Regarding Claim 7, Michener teaches and describes a data playback method for a data processor comprising:

a data storage device comprising cryptosystem means and a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity; and a data playback device for playing back data which is received from said data storage device (Column 4 lines 9 – 14), said data playback method comprising the steps of:

executing mutual authentication processing between said data storage device and said data playback device (Column 6 lines 33 – 45 and Column 7 lines 2 – 5), Michener teaches that mutual authentication between the user terminal and the storage with crypto unit;

when the mutual authentication is established, transmitting. from said data playback device to said data storage device, a set of storage-key-used CBC-mode-processing keys which is included in the header information of data stored in said data storage area and which is generated by executing encryption processing in the CBC

mode using a storage key unique to said data storage device (Column 6 lines 15 – 61 and Column 7 lines 2 – 5), Michener teaches that when the mutual authentication is established and that the transaction verification (session) keys are generated to be stored in the sectors;

decrypting, by said data storage device, the set of storage-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the storage key (Column 6 lines 21 – 25 and Column 7 lines 6 – 10);

transmitting, by said data storage device, to said data playback device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication encryption processing in the CBC mode on the set of decrypted storage-key-used CBC-mode-processing keys (Column 7 lines 6 – 10); and

obtaining, by said data playback device, a set of keys for decrypting encrypted sector data which is stored in each of the sectors in said data storage area by decrypting, in the CBC mode, the session-key-used CBC-mode-processing keys by using the session key (Column 6 lines 55 – 61 and Column 7 lines 2 – 9).

6. Regarding Claim 8, Michener teaches and describes a program providing medium for providing a computer program which controls a computer system to execute data recording processing for a data processor comprising:

a data storage device comprising cryptosystem means and a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which

each have a predetermined data capacity; and a data recording device for executing data storage processing by transmitting data to said data storage device (Column 4 lines 9 – 14); said computer program comprising the steps of:

executing mutual authentication processing between said data storage device and said data recording device (Column 6 lines 33 – 45 and Column 7 lines 2 – 5), Michener teaches that mutual authentication between the user terminal and the storage with crypto unit;

when the mutual authentication is established, transmitting, to said data storage device, by said data recording device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on said set of keys applicable to encryption processing on pieces of data to be stored in the sectors (Column 6 lines 15 – 61 and Column 7 lines 2 – 5), Michener teaches that when the mutual authentication is established and that the transaction verification (session) keys are generated to be stored in the sectors;

decrypting, by said data storage device, said set of session-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the session key (Column 6 lines 21 – 25 and Column 7 lines 6 – 10);

transmitting to said data storage device, a set of storage-key-used CBC-mode-processing keys which are generated by executing, based on a storage key unique to said data storage device, encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode-processing keys (Column 7 lines 6 – 10); and

generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys which are generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys, the header information corresponding to the data to be stored in said data storage device (Column 6 lines 16 – 28 and 48 – 61).

7. Regarding Claim 9, Michener teaches and describes a program providing medium for providing a computer program which controls a computer system to execute data playback processing for a data processor comprising:

a data storage device comprising cryptosystem means and a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity; and a data playback device for playing back data which is received from said data storage device (Column 4 lines 9 – 14); said computer program comprising the steps of:

executing mutual authentication processing between said data storage device and said data playback device (Column 6 lines 33 – 45 and Column 7 lines 2 – 5), Michener teaches that mutual authentication between the user terminal and the storage with crypto unit;

when the mutual authentication is established, transmitting, from said data playback device to said data storage device, a set of storage-key-used CBC-mode-processing keys which is included in the header information of data stored in said

generated by executing data storage area and which is encryption processing in the CBC mode using a storage key unique to said data storage device (Column 6 lines 15 – 61 and Column 7 lines 2 – 5), Michener teaches that when the mutual authentication is established and that the transaction verification (session) keys are generated to be stored in the sectors;

decrypting, by said data storage device, the set of storage-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the storage key (Column 6 lines 21 – 25 and Column 7 lines 6 – 10);

transmitting, by said data storage device, to said data playback device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on the set of decrypted storage-key-used CBC-mode-processing keys (Column 7 lines 6 – 10); and

obtaining, by said data playback device, a set of keys for decrypting encrypted sector data which is stored in each of the sectors in said data storage area by decrypting, in the CBC mode, the session-key-used CBC-mode-processing keys by using the session key (Column 6 lines 55 – 61 and Column 7 lines 2 – 9).

8. Claim 2 is rejected applied as above in rejecting Claim 1. Furthermore, Michener teaches and describes a data storage device wherein said cryptosystem means, generates key data as the header information of the data to be stored in said data storage area by using a storage key which is unique to said data storage device to

execute the encryption processing in the CBC mode on the received set of keys (Column 6 lines 16 – 28 and 48 – 61).

9. Claim 3 is rejected applied as above in rejecting Claim 1. Furthermore, Michener teaches and describes a data storage device wherein:

said data storage with said device capable of performing data communication with said data storage device (Column 4 lines 11 – 17);

the received set of keys is a set device performs mutual authentication of session-key-used CBC-mode-processing keys a session key generated in the mutual authentication (Column 6 lines 33 – 45 and Column 7 lines 2 – 5), Michener teaches that mutual authentication between the user terminal and the storage with crypto unit;

said cryptosystem means performs the decryption in the CBC mode of said set of encrypted session-key-used CBC-mode-encrypted in the CBC mode by using processing keys (Column 6 lines 21 – 25 and Column 7 lines 6 – 10); and

in said cryptosystem means CBC-mode-processing keys is generated by executing, based on a storage key unique to said data storage device, the encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode-processing keys, and said set of storage-key-used CBC-mode-processing keys is a set of storage-key-used transmitted as header-information-forming data to said device (Column 6 lines 16 – 28 and 48 – 61).

10. Claim 4 is rejected applied as above in rejecting Claim 1. Furthermore, Michener teaches and describes a data storage device wherein:

said data storage device performs mutual authentication with said device capable of performing data communication with said data storage device;

the received set of keys is header information on the data to be stored in said data storage area, and is a set of storage-key-used CBC-mode-processing keys encrypted in the CBC mode based on a storage key unique to said data storage device (Column 6 lines 33 – 45 and Column 7 lines 2 – 5), Michener teaches that mutual authentication between the user terminal and the storage with crypto unit;

said cryptosystem means performs the decryption in the CBC mode of the set of encrypted storage-key-used CBC-mode-processing keys by using said storage key (Column 6 lines 21 – 25 and Column 7 lines 6 – 10); and

in said cryptosystem means, a set of session-key-used CBC-mode-processing keys is generated by executing, based on a session key generated in the mutual authentication, the encryption processing in the CBC mode, and said set of session-key-used CBC-mode-processing keys is transmitted as data constituting decrypting key information (Column 6 lines 16 – 28 and 48 – 61).

11. Claim 5 is rejected applied as above in rejecting Claim 1. Furthermore, Michener teaches and describes a data storage device wherein:

from said device capable of performing data communication with said data storage device, said cryptosystem means receives: said set of keys correlated with the encryption keys or decryption keys for the sectors, as cryptosystem keys for performing cryptosystem processing on the data to be stored in said data storage area (Column 4 lines 11 – 17); and

an integrity-check-value generating key of data to be stored in at least one of the sectors (Column 6 lines 33 – 39, 62 – 65 and Column 8 lines 20 – 28); and

in said cryptosystem means, the received set of keys are encrypted in the CBC mode and are transmitted to said device (Column 6 lines 33 – 45 and Column 7 lines 2 – 5), Michener teaches that mutual authentication between the user terminal and the storage with crypto unit.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on Tuesday – Thursday 8:00a.m. To 3:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
February 21, 2005.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100